UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,795	06/15/2001	Yves Louis Gabriel Audebert	L741.01104	6672

7590 11/03/2006

STEVENS, DAVIS, MILLER & MOSHER, LLP
1615 L Street, N.W., Suite 850
Washington, DC 20036

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/880,795	AUDEBERT ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *41-71* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *41-71* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3, 8, 10/06*. 09/10/05
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Appeal Brief received on 08/09/06.

2. Claims 40-71 are pending.

Reopening of Prosecution

3. New Ground of Rejection After Appeal or Examiner's Rebuttal of Reply Brief In view of the Appeal Brief filed on 08/090/06, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below. To avoid abandonment of the application, appellant must exercise one of the following two options: (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or, (2) request reinstatement of the appeal. If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 40-41, 43, 45-61, 64-67, and 69-71 are rejected under 35 U.S.C. 102(e) as being anticipated by Andersson, US Publication No. 20020034301A1.

6. As per claims 40, 53-55, and 65:

Andersson discloses "A data processing system for performing authentications and business transactions comprising: at least one local client configured to support at least one network connection" in (Fig 1, PC 60, and Para 32),

> As is well known, a personal computer has the advantage, compared with current mobile devices, that it has a wider range of input options (such as a full size keyboard and a mouse), and has a larger display for retrieved data. Further, the personal computer 60 is provided with a wired broadband connection to the internet 50. Possible uses of a personal computer 60, in conjunction with the internet 50, include retrieving data from servers to which there is intended to be restricted access, and carrying out online transactions, which may include transmitting confidential user information to a third party computer. As described above, the third party computer, from which information is to be retrieved, or to which information is to be transmitted, has an associated authentication server 54.

"wherein a shared predetermined authentication policy is functionally stored in said at least one authentication server and said PSD" in (Para 0040-42);

> [0040] In outline, when the user first contacts the authentication server 54, the authentication server issues a challenge to the user. **The authentication token encrypts the challenge with the user's private key, and returns it to the authentication server. The returned challenge is then decrypted by the authentication server with the user's public key, and the authentication server verifies that the decrypted challenge is the same as the original challenge.**
>
> [0041] Thus, there is no requirement for a user to enter a password to be able to access confidential information which is on the authentication server 54. The necessary password can in effect be generated automatically by the WAP-enabled device 10, **using the public key infrastructure provided by the cryptographic module of the device, on the basis of the identity of the user confirmed by the wireless identity module in the device.**
>
> [0042] In this way, **the WAP-enabled device 10 can be used an authentication token for multiple authentication servers, including authentication servers from multiple manufacturers**. All that is necessary is for an authentication server and the device 10 to be able to operate the same authentication protocols.

"at least one authentication server configured to perform authentications according to a predetermined authentication policy and further configured to support at least one network connection" in (Para 0040-42);

"an intelligent portable device configured to support a PSD, at least one device connection and at least one network connection" in (Para 20-21); and

> [0020] For example, **the cryptographic module can be realized in hardware or in software in the phone 10, or may be provided on an external smart card**, or the phone 10 may also include a Wireless Identity Module (WIM) card, which is used to identify the subscriber.
>
> [0021] In accordance with preferred embodiments of the present invention, the cryptographic module of the phone, and other features which are used to provide secure communication using the Wireless Application Protocol, also **allow the phone 10 to be used as an authentication token for other communications**.

"a PSD which is functionally connected to said intelligent portable device and configured to generate authentication information according to said predetermined authentication policy, and which is associated to an identified user" in (Para 27-28),

> [0027] At step 74, **the device verifies the identity of the user**. As part of this procedure, the device gives a prompt to the user, asking the user to identify himself. One possibility is to require **the user to enter a Personal Identification Number (PIN)**. However, to provide an additional layer of security, the device 10 can also use a form of biometrics to provide user authentication.

> Thus, for example, the device 10 can include **means for examining a physical feature which uniquely or nearly uniquely identifies a user**, such as his fingerprints or voice recognition or another biometric technique, and **allowing the user access to the system only if that physical feature is found to match the intended user**.
>
> [0028] Once **the user has authenticated himself to the token, the token can authenticate itself to the modem 15, at step 76. Thus, using a selected authentication protocol, the token performs the necessary calculations, and, at step 78, information is provided to the WAP browser software, for example allowing it to respond to challenges from the authentication server 17, or to generate a password based on offline information**.

"wherein: said at least one local client and said at least one authentication server are functionally connected to each other over at least one network connection" in (Para 33),

> [0033] Also, FIG. 2 shows the **PC connected to the internet 50 through a modem 56, which has an associated authentication server 58**. The description below refers to authentication towards the authentication server, but the same procedure can be used to authenticate towards the authentication server 58.

said predetermined authentication policy is functionally stored within said PSD and said at least one authentication server" in (Para 0040), and

"said at least one local client comprises an activator of an authentication according to said authentication policy between said PSD and said at least one authentication server upon an action of said identified user on said at least one local client" in (Para 0047).

> [0047] When used with a personal computer in this way, **commands may be transferred to and from the device using the AT protocol**. Thus, for example, **passwords which are generated in the mobile phone 10 acting a the authentication token are transferred to the personal computer 60**, and can be automatically sent to the **authentication server**.

7. As per claims 41 and 66-67:

Andersson discloses "The data processing system according to claims 40 and 65, wherein: said at least one local client is configured to support at least one device connection" in (Para 45); and

> [0045] In the case where the device 10 is used as an authentication token for a personal computer, described above with reference to FIG. 3, there is preferably a connection between the personal computer 60 and the WAP-enabled mobile phone 10. **The connection may be wired, or, advantageously, communications between the personal computer 60 and mobile phone 10 can take place using the Bluetooth short-range radio transmission protocol.**

said intelligent portable device is functionally connected to said at least one local client through said at least one device connection of said at least one local client and further configured as a hardware device peripheral which allows the PSD to communicate said authentication information to said at least one authentication server using said at least one network connection of said at least one local client" in (Para 47).

> [0045] In the case where the device 10 is used as an authentication token for a personal computer, described above with reference to FIG. 3, there is preferably a connection between the personal computer 60 and the WAP-enabled mobile phone 10. **The connection may be wired, or, advantageously, communications between the personal computer 60 and mobile phone 10 can take place using the Bluetooth short-range radio transmission protocol.**

8. As per claim 43:

Andersson discloses ""The data processing system according to claim 40, wherein said predetermined authentication policy includes asynchronous authentication means, synchronous authentication means and cryptography means" in (Para 40-41). [Asynchronous authentication means is authentication challenge exchanging from the server to device back and forth. Synchronous authentication is the token

authentication. And final cryptographic means is the encryption method.] (See the application specification on page 3)

> In asynchronous authentication methods, typically a client requests access to information contained on a server, the server generates a challenge to the client and the client generates a response, which is validated by the server.
>
> In synchronous authentication methods, one-time password challenges are independently generated by a client and a server utilizing a common stand, incrementing variables and a shared secret symmetrical key and compared by the server.

9. As per claim 45:

Andersson discloses "The data processing system according to claim 40, wherein said intelligent portable device is functionally connected to said at least one authentication server through at least one network connection and configured as an independent portable device which allows the PSD to communicate said authentication information to said at least one authentication server using said at least one network connection" in (Para 0040).

> [0040] In outline, when the user first contacts the authentication server 54, the authentication server issues a challenge to the user. The authentication token encrypts the challenge with the user's private key, and returns it to the authentication server. The returned challenge is then decrypted by the authentication server with the user's public key, and the authentication server verifies that the decrypted challenge is the same as the original challenge.

10. As per claim 46:

Andersson discloses "The data processing system according to claim 45, wherein said at least one network connection between said at least one authentication server and said intelligent portable device is selected from the group consisting of a wireless RF network and a digital cellular network" in (Para 0012-16) [WAP protocol is implemented in GSM, CDMA, or even G2 environment].

11. As per claims 47:

Andersson discloses "The data processing system according to claim 45, wherein said intelligent portable device is functionally connected to said at least one authentication server through at least two network connections over at least two networks, a first network connection being dedicated for sending a first portion of said authentication information and a second network connection being dedicated for sending a second portion of said authentication information" in (Fig 1, Modem 15 and Modem 56).

12. As per claim 48:

Andersson discloses "The data processing system according to claim 40, wherein a plurality of network and device connections are facilitated using said intelligent portable device" in (Fig 1, Para 0012).

13. As per claim 49:

Andersson discloses "The data processing system according to claim 40, wherein said intelligent portable device is configured as a hardware device peripheral" in (Para 20).

14. As per claim 50:

Andersson discloses "The data processing system according to claim 40, wherein said intelligent portable device is configured as an independent intelligent portable device" in (Para 0012).

15. As per claim 51:

Andersson discloses "The data processing system according to claim 40, wherein said predetermined authentication policy includes asynchronous authentication means and cryptography means" in (Para 0040).

16. As per claim 52:

Andersson discloses "The data processing system according to claim 40, wherein said predetermined authentication policy includes synchronous authentication means and cryptography means" in (Para 0040).

17. As per claim 56:

Andersson discloses "The method according to claim 54, wherein said at least one unique identifier is used by said at least one authentication server for locating and communicating with another intelligent portable device associated with a second level approver" in (Para 0027).

18. As per claim 57:

Andersson discloses "The method according to claim 53, wherein a plurality of authentications are facilitated using said shared predetermined authentication policy" in (Para 0027-28).

19. As per claim 58:

Andersson discloses "The method according to claim 53, further comprising an authentication of said identified user to said PSD by entry of a Personal Identification Number" in (Para 027).

20. As per claim 59:

Andersson discloses "The method according to claim 53, further comprising an authentication of said identified user to said PSD by entry of a biometric result" in (Para 0027).

21. As per claim 60:

Andersson discloses "The method according to claim 58 or 59, wherein said entry is conducted using a user interface and display associated with said intelligent portable device" in (Para 0027, and 0016).

> [0016] As is known, content on web pages which are intended to be accessed by web-enabled devices is conventionally written using Wireless Markup Language (WML), a language which is designed to meet the constraints which typically apply in this environment, namely the relatively low bandwidth available in the wireless interface, and the **generally small available display sizes on the handheld WAP-enabled devices such as mobile phones**.

22. As per claim 61:

Andersson discloses "The method according to claim 58 or 59, wherein said entry is conducted using a user interface and display associated with said at least one local client" in (Para 0032, and 0048).

> [0048] However, a manual operation is also possible, in which the necessary authentication calculations are carried out in the authentication token, and the required password or passwords are displayed on a screen of the device, and **can be manually entered by the user through the keyboard of the personal computer, and can then be sent to the authentication server**.

23. As per claim 64:

Andersson discloses "The method according to claim 53, further comprising business transactions" in (Para 0013) [Authentication method in the invention to allow the user to access information from web pages].

24. As per claim 69:

Andersson discloses "The intelligent portable data processing device according to claim 65 or 68, functionally connected to a plurality of authentication servers using said at least one network connection" in (Fig 1).

25. As per claims 70-71:

Andersson discloses "The intelligent portable data processing device according to claim 65, wherein the PSD is a physical device" in (Para 0020, Smart card).

Claim Rejections - 35 USC § 103

26. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 42, 44, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson, in view of Ortiz et al, US Publication No. 20020042774A1, hereinafter "Ortiz".

28. As per claim 42:

Andersson discloses "The data processing system according to claim 41, wherein said device connection between said at least one local client and said intelligent portable device is selected from the group consisting of a direct connection, an optical connection, a wireless RP connection or an electro-acoustical connection" in (Para 45).

However, Andersson does not specifically disclose the implementation of an optical connection for connecting the device to the local client.

Nevertheless, Ortiz discloses a method of implementing a smart card attached to a PDA cablable of connecting to a KIOSH (PC) by infrared, bluetooth, wireless, and docking station connection to carry out a business transaction to a remote server in (Para 0097).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Andersson's invention to incorporate the group of connections specified in Ortiz's invention to allow the flexibility of connecting two devices.

29. As per claims 44 and 68:

Andersson discloses "The data processing system according to claims 40 and 65, comprising at least two local clients (PC 60) respectively functionally connected to at least two authentication servers (Authentication Server 54 and 56) over at least one network connection, wherein each of said at least two local clients is configured to support at least one device connection, and wherein said intelligent portable device is functionally connected (Para 0045) to each of said at least two local clients through said at least one device connection of each of said at least two local clients and further configured as a hardware device peripheral" in (Para 33-34).

However, Andersson does not specifically disclose the implementation of multiple clients.

Nevertheless, Ortiz does disclose multiple PCs as kioskes for the customer with portable devices connecting to the kioskes for business transactions in (Para 0077-0078).

> [0078] Port 12 may be connected to CPU 10 and can be temporarily attached, for example, to a docking station to transmit information to and from hand held device 11 to other devices, such as **personal computers, retail cash registers, electronic kiosk devices**, and so forth. Port 12 can also be configured, for example, to link with a modem, cradle or docking station, which are well known
> in the art, that permit network devices, a personal computer or other computing devices to communicate with hand held device 11.

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Andersson's invention to incorporate Ortiz's teaching of implementing multiple kiosks for multiple customer transaction using the portable devices.

30. Claim 62 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Kortesalmi et al, US Patent No. 6427073B1, hereinafter "Kortesalmi".

31. As per claim 62:

Andersson does not disclose "The method according to claim 58 or 59, wherein exceeding a maximum number of attempts at authentication ends the authentication".

Nevertheless, Kortesalmi discloses "Preventing Misuse of a Copied Subscriber Identity in a Mobile Communication System" invention, which includes a method of ending the authentication process by block the access to the SIM or Smart card in (Col 3 lines 40-47).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Andersson's invention to incorporate the protection mechanism in the authentication process to protect unauthorized access to the portable device.

32. Claim 63 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andersson in view of Otway et al, US Patent No. 7020773B1, hereinafter "Otway".

33. As per claim 63:

Andersson discloses "the method according to claim 53, wherein said shared predetermined authentication policy includes asynchronous authentication and cryptography".

However, Andersson does not explicitly teach "wherein exceeding a predetermined response time ends the authentication".

Nevertheless, Otway discloses the "Strong Mutual Authentication of Devices", which includes a method of authenticating a client with smart card to a remote server over a communication connection synchronously" in (Col 1 lines 10-30). The client transmit authentication information back and forth with the server within a time interval. A timeout period is set for the client to response to a challenge (Col 6 lines 9-15).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Andersson's invention to incorporate Otway's disclosure of implementing a timeout period for responding to prevent fraudulent.

34. **Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).**

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KAMBIZ ZAND
PRIMARY EXAMINER

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100